UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,772	07/21/2000	Raynold M. Kahn	PD-200045	3987

20991 7590 01/23/2008

THE DIRECTV GROUP, INC.
PATENT DOCKET ADMINISTRATION
CA / LA1 / A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
01/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/620,772	KAHN ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-17,19-29,31-50, 52 and 53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-17,19-29,31-50, 52 and 53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *Nov. & Dec. 2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication filed on: 26 October 2007 with acknowledgement of an original application filed on 21 July 2000.

2. Claims 1, 2, 4-17, 19-29, 31-50, 52, and 53, are pending; claims 1, 17, and 28 are independent claims. Claims 1 and 17 have been amended. Claim 52 and 53 are new. Claims 3, 18, 30, and 51 have been canceled. Amendments to the claims are accepted.

3. The IDS submitted 29 November 2007 and 6 December 2007 have been considered.

Response to Arguments

4. Applicant's arguments filed 26 October 2007 have been fully considered however they are not persuasive or moot due to new grounds of rejection below.

I) In response to applicant's arguments on page 17, *"The Applicant's invention differs from the related prior art that the Applicant is aware of in that it encrypts the second (CP) encryption key in the condition access module instead of the receiver, and does so using a n key (CAM key) that is generated or stored internal to the CAM".*

The Examiner disagrees with the argument for multiple reasons. First the applicant's arguments are not specifically stated in the claims, the claim does not indicate that a second key is stored in the CAM. Second the applicant is considering the references individual not in combination. Okabe teaches that a key can be stored in a receiver. Downs teaches the distribution of Secure Containers (SC) technology. In Downs the receiver of a SC whether a vendor, distributor, or user computer has the ability to re-encrypt the media to a second, third, and fourth encryption keys.

II) In response to applicant's argument beginning on page 17, *"Claim 1 allocates functions between the receiver in the CAM. Namely, it specifies that: ... The conditional access module does not: store the re-encrypted program material and the fourth encryption key ... Returning to the cited references, we note that Downs discloses no function allocation between hardware elements at all ... all functions are performed by the user's computer ... Okabe is of no help. As described below, it discloses a system in which the terminal (which the Office Action analogizes to the Applicant's CAM) ... These functions are not analogous those recited in claim 1 (where nothing is "further encrypted", but rather decrypted and re-encrypted.)".*

The Examiner disagrees with argument for multiple reasons. Again the applicant is placing limitation that are not present in the claims, the negative limitation argued "that the conditional access module does not store the re-encrypted program material and the fourth encryption key" is not in the claims. Plus the argument does not make sense, obviously if the CAM produces the re-encrypted program material and the fourth encryption key then provides them for storage at some point it has the re-encrypted program material and the fourth encryption key are stored in the CAM registers. Second Okabe and Downs are analogous art both are directed to digital rights management (DRM). Third although applicant is claiming the encryption is done in the conditional access module (CAM) not in a computer like Downs, obviously to do encryption the CAM must contain a CPU just like a computer contains a CPU. Fourth the applicant is placing limitation not in the claims as well as not considering the entire references of Okabe and Downs both disclose hardware elements, see Okabe col. 6, lines 34-60 which teaches that the content sale system includes a terminal apparatus 5 located in a store (for example, a kiosk or a convenience store). The terminal apparatus includes a computer,

communication devices, and an interface for connection with a customer's player. Also see Downs col. 6, lines 59- for an example of the hardware that can receive SC. The applicant's description as well as claimed limitation of the conditional access module (CAM) do not limit the CAM from being a kiosk in a store that the provides a user's player or receiver with encrypted access control information.

III) In response to applicant's argument beginning on page 19, *"It would also not be obvious to modify the Okabe and Downs combination to arrive at the Application's invention ... As a threshold matter, the prior art teaches a different functional allocation than that which is claimed by the Applicant"*.

The Examiner disagrees with argument the applicant's claimed disclosure as well as the prior art references both are directed to digital rights management by encrypting access control information. The KSR ruling indicates it is permissible to combine prior art references from the same endeavor.

IV) In response to applicant's explanation of the system described in EP 0 989 557 on pages 19-23, this is irrelevant because as previously noted Okabe and Downs teach the claimed limitations. The EP was not utilized in the rejection; therefore all arguments that address the improvements by the applicant's claimed invention are irrelevant. The 'CAM' comprising a smartcard was not introduced until dependent claim 4. This limitation is taught with the combination of Dolphin US Patent 5,677,953.

VI) In response to applicant's argument beginning on page 23, *"Finally, the Office Action offers the following motivation to combine Okabe and Downs references: ... This provides a generalized motivation to provide for digital rights (something that both Okabe and*

Downs provide already individually), but does not explain why one would modify Okabe as described in Downs or Downs as described in Okabe".

The Examiner disagrees with argument the applicant's claimed disclosure as well as the prior art references both are directed to digital rights management by encrypting access control information. As stated above the KSR ruling indicates it is permissible to combine prior art references from the same endeavor.

VII) In response to applicant's arguments on page 25, *"... in further view of Dolphin ... Applicants respectfully traverse these rejection for the reasons described above with respect to the independent claims".*

The Examiner disagrees as previously stated Downs and Okabe teach the claimed independent claims. Also as previously stated all prior art cited directed to DRM therefore they are directed to the same field of endeavor, according to KSR rule it is permissible to combine the references.

VIII) In response to applicant's argument beginning on page 25, *"In paragraph (8), the Office Action rejected claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50 under ... in further view of Akins ... Applicants respectfully traverse these rejections. With Respect to Claims 6, 44-50: Claim 6 recites that the second encryption key is generated at least in part from the metadata ... Respectfully, this only discloses the use of a control word to determine whether the subscriber is entitled to view a program. It does not even remotely disclose generating the second encryption key at least in part from the metadata. Further, the motivation to modify Okabe and Downs as described in Akins (more flexibility) doesn't explain how any suggested change would increase flexibility. There is a significant advantage in generating the second key at least in part from the*

metadata. It prevents having to generate a random number for the second key, and also assures that the metadata can be later recovered."

The Examiner disagrees with the argument for multiple reasons. One using the broadest reasonable interpretation the 'metadata' was interpreted to be the Entitlement Control Messages which is used by the decryptor to produce a key. Second Akins is directed to DRM as well therefore according to KSR ruling it is permissible to combine the references. Finally the advantages stated in the arguments are not placed in the claims, therefore these arguments are irrelevant.

VIII) In response to applicant's argument beginning on page 26, *"With Respect to Claim 13: Claim 13 recites: The method of claim 12, wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein the second encryption key and the third encryption key are stored in a smartcard ... None of the cited references discloses the functional allocation presented in claim 13".*

The Examiner disagrees with the argument for multiple reasons. One the references should be looked at in combination. Second the entire references should be considered. Akins teaches in col. 21, lines 1-40 that the encryption and decryption and all the components of DHCTSE can be performed in a smartcard. The pre-buy message is taught in Akins col. 12, lines 39-67.

IX) In response to the applicant's arguments that the dependent claims and new claims are also allowable. The Examiner disagrees as stated above the applied prior art references teach the claimed subject matter.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1, 5, 14-18, 20, 25-28, 32, 34, 36, 40-43, 52 and 53,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Okabe et al. US Patent No. 6,889,208 (hereinafter '208) in view of Downs et al US Patent No. 6,574,609 (hereinafter '609).

As to independent claim 1, "A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:" is taught in '208 col. 7, lines 13-25;

"(b) decrypting the received access control information in a conditional access module releasably coupleable with the receive to produce the first encryption key" is shown in '208 col. 7, lines 34-48;

the following is not explicitly taught in '208:

"(a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data" however '609 teaches that program material is encrypted in a Secure Container that includes encrypted program material as well as

access control information, i.e. usage conditions that is encrypted according to a first encryption key in col. 10, lines 5-17;

"(c) decrypting the program material in the receiver using the first encryption key" however '609 teaches that program material can be decrypted in user devices in col. 11, line 64 through col. 12, line 11;

"(d) re-encrypting the program material according to a second encryption key; and" however '609 teaches that the End-User devices enforce usage conditions before copying to an external device in col. 20, lines 10-29;

"(e) encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; (f) providing the re-encrypted program material and the fourth encryption key for storage external to the conditional access module" however '609 teaches that when a copy is generated a new encryption key is made in col. 20, lines 30-50.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated. One of ordinary skill in the art would have been motivated to perform such a modification because content distributors have been slow to embrace digital content distributions systems because of the lack of security for digital content see '609 (col. 2, lines 2-44) "The use of global distribution systems such as the Internet for distribution of digital assets such as music, film, computer programs, pictures, games and other content continues to grow. At the same time owners and publishers of valuable digital content have been slow to embrace the use of the Internet for distribution of digital assets for several reasons. One reason is that owners are afraid of unauthorized copying or pirating of digital

content. The electronic delivery of digital content removes several barriers to pirating ... This degradation in quality is not present when a picture is stored digitally. Each copy, and every generation of copies can be as clear and crisp as the original. The aggregate effect of perfect digital copies combined with the very low cost to distribute content electronically and to distribute content widely over the Internet makes it relatively easy pirate and distribute unauthorized copies. With a couple of keystrokes, a pirate can send hundred or even of thousands of perfect copies of digital content over the Internet. Therefore a need exists to ensure the protection and security of digital assets distributed electronically. Providers of digital content desire to establish a secure, global distribution system for digital content that protects the rights of content owners. The problems with establishing a digital content distribution system includes developing systems for digital content electronic distribution, rights management, and asset protection".

As to dependent claim 5, "wherein the access control information further comprises metadata describing at least one right for the program material" however '609 teaches the Secure Container incorporates various usage conditions in col. 9, lines 45-60, note 'a usage condition' is interpreted to be equivalent to 'at least one right for the program material'. The motivation to combine '609 and '208 is the same as stated above in claim 1.

As to dependent claim 14, "wherein the re-encrypted program material and the fourth encryption key are stored on a media storage device" however '609 teaches that when a copy is generated a new encryption key is made in col. 20, lines 30-50. The motivation to combine '609 and '208 is the same as stated above in claim 1.

As to dependent claim 15, "wherein the control data is temporally-variant" however '609 teaches that the usage conditions can have a time period associated with validity in col. 10, lines 39-43. The motivation to combine '609 and '208 is the same as stated above in claim 1.

As to dependent claim 16, "wherein the temporally-variant control data associates an expiration time with the program material" however '609 teaches that the usage conditions can have a time period associated with validity in col. 10, lines 39-43. The motivation to combine '609 and '208 is the same as stated above in claim 1.

As to independent claim 17, "An apparatus for storing program material encrypted according to first encryption key for replay, comprising:" is taught in '208 col. 7, lines 13-25;

"for decrypting the access control information to produce the first encryption key" and **"wherein the conditional access module is releasable communicatively coupled to a tuner, the tuner to enable reception of the encrypted access control information and program material encrypted according to a first encryption key"** is shown in '208 col. 7, lines 34-48;

the following is not explicitly taught in '208:

"a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising: a first decryption module" however '609 teaches that program material is encrypted in a Secure Container that includes encrypted program material as well as access control information, i.e. usage conditions that is encrypted according to a first encryption key in col. 10, lines 5-17;

"a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and a second decryption module for decrypting the fourth encryption key to produce the second encryption key, the tuner comprising: a third decryption module, for decryption the program material using the first encryption key produced by the condition access module; a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key" however '609 teaches that when a copy is generated a new encryption key is made in col. 20, lines 30-50, it is obvious that the amount of keys is dependent upon the usage condition contained within the SC.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated. One of ordinary skill in the art would have been motivated to perform such a modification because content distributors have been slow to embrace digital content distributions systems because of the lack of security for digital content see '609 (col. 2, lines 2-44) "The use of global distribution systems such as the Internet for distribution of digital assets such as music, film, computer programs, pictures, games and other content continues to grow. At the same time owners and publishers of valuable digital content have been slow to embrace the use of the Internet for distribution of digital assets for several reasons. One reason is that owners are afraid of unauthorized copying or pirating of digital content. The electronic delivery of digital content removes several barriers to pirating ... This degradation in quality is not present when a picture is stored digitally. Each copy, and every

generation of copies can be as clear and crisp as the original. The aggregate effect of perfect digital copies combined with the very low cost to distribute content electronically and to distribute content widely over the Internet makes it relatively easy pirate and distribute unauthorized copies. With a couple of keystrokes, a pirate can send hundred or even of thousands of perfect copies of digital content over the Internet. Therefore a need exists to ensure the protection and security of digital assets distributed electronically. Providers of digital content desire to establish a secure, global distribution system for digital content that protects the rights of content owners. The problems with establishing a digital content distribution system includes developing systems for digital content electronic distribution, rights management, and asset protection".

As to dependent claim 18, further comprising: a tuner, communicatively coupleable to the conditional access module for receiving the encrypted access control information and the program material encrypted according to a first encryption key" is shown in '208 col. 6, lines 34-48 (Note tuner is considered equivalent to a communication device that communicates with a satellite);

"a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module; a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key" however '609 teaches that when a copy is generated a new encryption key is made in col. 20, lines 30-50.

As to dependent claim 20, this claim contains substantially similar subject matter as claim 5; therefore it is rejected along similar rationale.

As to dependent claim 25, "wherein the second encryption key is stored in the conditional access module" is taught in '208 col. 7, lines 13-38.

As to dependent claim 26, "wherein the third encryption key is stored in the conditional access module" is shown in '208 col. 7, lines 13-38.

As to dependent claim 27, "wherein the conditional access module is releaseably communicative coupleable to: a tuner for receiving the encrypted access control information and the program material encrypted according to a first encryption key" is taught in '208 col. 6, lines 33-48;

"a third decryption module, for decrypting the program material using the first encryption key from the conditional access module a second encryption module, for re-encrypting the decrypted program material according to the key and a media storage device" however '609 teaches that when a copy is generated a new encryption key is made, in addition '609 teaches if allowed the copy can be to a media storage device in col. 20, lines 30-50.

As to independent claim 28, this claim is directed to the apparatus implementing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claims 32, this claim contains substantially similar subject matter as claim 5; therefore it is rejected along similar rationale.

As to dependent claim 34, "further comprising: means for generating replay right data from the metadata" however '609 teaches that the metadata contains in it the usage

conditions in col. 10, lines 5-17, note these usage condition are equivalent to the 'replay right data' the means for generating is by using the Secure Container technology taught in '609.

As to dependent claim 36, "further comprising: means for retrieving the stored re-encrypted program material and the fourth encryption key; means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key, and means for decrypting the re-encrypted material using the second encryption key" however '609 teaches that when a copy is generated a new encryption key is made in col. 20, lines 30-50.

As to dependent claim 40-43, these claim contain substantially similar subject matter as claims 14-16; therefore they are rejected along similar rationale.

As to dependent claim 52 and 53, "wherein the second encryption key is stored in the conditional access module" however '609 teaches that encryption keys and stored in a content hosting site in col. 10, lines 5-8.

7. **Claims 2, 4, 29, and 31,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Okabe et al. US Patent No. 6,889,208 (hereinafter '208) in view of Downs et al US Patent No. 6,574,609 (hereinafter '609) in further view of Dolphin US Patent No. 5,677,953 (hereinafter '953).

As to dependent claim 2, the following is not taught in the combination of teachings of '609 and '208: **"wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of: decrypting the received access control information to produce the temporally variant control data; and modifying the temporally variant control data to generate temporally-invariant control**

data" however '953 teaches that an attribute can be assigned to a decrypted content such as the time period the decryption key is valid for in col. 7, lines 7-11, in addition the usage conditions can be modified in col. 7, line 36 through col. 8, line 26.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 and '609 to include a means to update the time variant control data. One of ordinary skill in the art would have been motivated to perform such a modification because a need exists for subscribers to update their subscription services when the service is terminated due to time limit see '953 (col. 2, lines 22 et seq.) "The need for protection of information stored on, for example, CD-ROMs, or one a local or remote server from unauthorized access needs to be satisfied before such a publication distribution system is acceptable to publishers. Security provided at both the publisher's site and subscriber's site is needed to prevent the unauthorized access to data contained on the media. Moreover, valid subscribers need to be protected when their subscription service is terminated".

As to dependent claim 4, "wherein the conditional access module on a smartcard" however '953 teaches the invention includes utilization of an encryption tool such as a smartcard in col. 2, lines 59-67. The motivation to combine '208, '609, and '953 is the same as stated above in claim 2.

As to dependent claims 29 and 31, these claims contain substantially similar subject matter as claims 2 and 4; therefore they are rejected along similar rationale.

8. **Claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50** are rejected under 35 U.S.C. 103(a) as being unpatentable over Okabe et al. US Patent No. 6,889,208 (hereinafter '208) in view of

Downs et al US Patent No. 6,574,609 (hereinafter '609) in further view of Akins, III et al. U.S. Patent No. 6,560,340 (hereinafter '340).

As to dependent claim 6, the following is not explicitly taught in the combination of '208 and '609: **"further comprising the step of generating the second encryption key at least in part from the metadata"** however '340 teaches that data distributed with the content such as a 'entitlement control messages' may include a key or control word for what programs the subscriber is allowed to view in col. 4, lines 50-61.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 and '609 to include an improved means of distributing content data. One of ordinary skill in the art would have been motivated to perform such a modification because more flexible means are needed to distribute data see '340 (col. 2, lines 60 et seq.) "Thus, the service distribution organizations require access restrictions which are both more secure and more flexible than those in conventional systems.

As to dependent claim 7, "wherein steps (b)-(f) are performed in response to a pre-buy Message" however '340 teaches in col. 12, lines 39-67. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 8, "wherein the access control information further comprises metadata describing at least one right for the program material and the method further comprises the step of: generating replay right data from the metadata" however '340 teaches in col. 31, lines 7-24. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 9, "wherein the replay right dam is further generated from pre-buy data" however '340 teaches in col. 31, lines 7-24. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 10, "further comprising the steps of retrieving the stored re-encrypted program material and the fourth encryption key; decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and decrypting the re-encrypted material using the second encryption key" however '340 teaches in col. 6, lines 24-53. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 11, "wherein the step of decrypting the fourth encryption key using the third encryption key to produce the second encryption key is performed in response to a subscriber request to access the program material" however '340 teaches in col. 30, lines 38-67. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 12, "wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the method further comprises the steps of; generating replay right data from the metadata; accepting the buy data; comparing the buy data with the replay right data; and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data" however '340

col. 12, line 56 through col. 13, line 39. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 13, "wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein: the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata sued the pie-buy message in the smartcard; and the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data arid the replay right data tire performed in the smartcard" however '340 teaches in col. 21, lines 1-40. The motivation to combine '340, '609, and 208 is the same as stated above in claim 6.

As to dependent claim 19, "wherein the conditional access module further comprises: a pre-buy module, for controlling the first decryption module" however '340 teaches in col. 12, line 56 through col. 13, line 14. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 21, "wherein pre-buy module generates replay right data from the metadata" however '340 teaches the use of impulse pay per view message, the pay per view messages are received by the set top box, which obviously is the 'pre-buy module' in col. 12, lines 39-67. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 22, "further comprising a buy module, communicatively coupled to the pre-buy module" however '340 teaches the use of impulse pay per view

message, the pay per view messages are received by the set top box, which obviously is the 'pre-buy module' in col. 12, lines 39-67. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 23, "wherein the buy module comprises: a purchase module; for accepting buy data, and comparing the buy data and the replay right data from the pre-buy module; and a control module for controlling the second decryption module based on the comparison between the buy data and the replay right data" however '340 teaches that the messages receive works with the delivery system and entitlement agents in col. 13, lines 14-54. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 24, "further comprising a billing module, for recording the buy data" however '340 teaches the entitlement agent responds to the FPM by adjusting its billing as required in col. 40, lines 2-5. The motivation to combine '340, '609 and '208 is the same as stated above in claim 6.

As to dependent claim 44, "wherein the access control information further comprise metadata and the method further comprises the step of generating the second encryption key at least in part from metadata" however '340 teaches generating keys from the metadata received in col. 4, lines 50-61.

As to dependent claim 45, "further comprising the step of: augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" however '340 teaches using the metadata received to update the control information in col. 4, lines 50-61.

As to dependent claim 46, "wherein the access control information further comprises metadata describing at least one right for the program material and the method further comprises the step of : augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" however '340 teaches the metadata consist of program access rights and that these access rights can be used before encryption in col. 4, lines 50-61.

As to dependent claims 31-42, these claims contain substantially similar subject matter as claims 4-16, and 44-46; therefore they are rejected along similar rationale.

As to dependent claim 47, "wherein the conditional access module generates the second encryption key at least in part from the metadata" however '340 teaches in col. 4, lines 50-61. The motivation to combine '208 and '340 is the same as stated above in claim 17.

As to dependent claim 48, "wherein the access control information further comprises a metadata and the conditional access module generated the second encryption key at least in part from the metadata" however '340 teaches in col. 4, lines 50-61.

As to dependent claim 49, "wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" is taught in '208 col. 7, lines 13-25.

As to dependent claim 50, "wherein the access control information further comprises metadata, and wherein the conditional access module augments the second encryption key with at least a portion of the metadata before encrypting the second encryption key in the conditional access module" however '340 teaches in col. 4, lines 50-61. The motivation to combine '208 and '340 is the same as stated above in claim 17.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
18 January 2008